ITRM Standard SEC502-00
Effective Date: July 1, 2006
Revised Date: January 11, 2007

COMMONWEALTH OF VIRGINIA

Information Technology Resource Management

INFORMATION TECHNOLOGY SECURITY AUDIT STANDARD

Virginia Information Technologies Agency (VITA)

ITRM PUBLICATION VERSION CONTROL

ITRM Publication Version Control: It is the User's responsibility to ensure they have the latest version of this ITRM publication. Questions should be directed to VITA's Associate Director for Policy, Practice and Architecture (PPA) within the Technology Strategies and Solutions (TSS) Directorate. PPA will issue a Change Notice Alert, post it on the VITA Web site, and provide an e-mail announcement to the Agency Information Technology Resources (AITRs) and Information Security Officers (ISOs) at all state agencies and institutions as well as other parties PPA considers to be interested in the change.

This chart contains a history of this ITRM publication's revisions.

Version	Date	Purpose of Revision
Original	July 1, 2006	Base Document
	October 17, 2006	Minor wording changes. No impact on the intent of this standard.
Revision 1	January 11, 2007	Performance of a "Risk Assessment (RA)" as the basis for developing audit plans was included in the original standard because of an oversight. This revision corrects that oversight by deleting references to "Risk Assessment (RA)" on pages iii (**Purpose)** and 3 (**2.1 – Planning for IT Security Audits**).

PREFACE

Publication Designation

ITRM Standard SEC502-00

Subject

Information Technology Security Audit Standard

Effective Date

July 1, 2006

Revised Date

January 11, 2007

Compliance Date

February 1, 2007

Supersedes

None

Scheduled VITA Review:

One (1) year from the effective date, then every two years thereafter.

Value Statement

Agencies are continuously seeking ways to better secure their databases and data communications that are vital to fulfilling their missions and achieving desired program results. A key factor in helping achieve such outcomes and minimizing operational problems is to implement appropriate internal control. This standard enhances data security by proactively assessing that appropriate IT security controls exist around government databases and data communications.

Authority

Code of Virginia, §§ 2.2-2005 – 2.2-2032.
(Creation of the Virginia Information Technologies Agency; "VITA;" Appointment of Chief Information Officer (CIO).

Scope

This standard is applicable to all State agencies and institutions of higher education (collectively referred to as "Agency") that manage, develop, purchase, and use information technology databases or data communications in the Commonwealth. Academic "instruction or research" systems, however, are exempt from this *Standard*. This exemption, does not, however, relieve these academic "instruction or research" systems from meeting the requirements of any other State or Federal Law or Act to which they are subject. This *Standard* is offered only as guidance to local government entities.

Purpose

This standard delineates the methodology for conducting an IT security audit of sensitive government databases and data communications systems that contain Agency information as identified and prioritized in an Agency's Business Impact Analysis.

Responsibilities

(Italics indicate quote from the Code of Virginia requirements)

Chief Information Officer
In accordance with *Code of Virginia* § 2.2-2009, the Chief Information Officer (CIO) is assigned the following duties: *"The CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government databases and data communications. At a minimum, these policies, procedures and standards shall address the scope of security audits and which public bodies are authorized to conduct security audits."*

Council on Technology Services
In accordance with the *Code of Virginia* § 2.2-2009, the Council on Technology Services is assigned the following duties: *"In developing and updating such policies, procedures and standards, the CIO shall consider, at a minimum, the advice and recommendations of the Council on Technology Services."*

Technology Strategies and Solutions Directorate
In accordance with the *Code of Virginia* § 2.2-2010, the CIO has assigned the Technology Strategies and Solutions Directorate the following duties: *"Develop and adopt policies, standards, and guidelines for managing information technology by state agencies and institutions*."

All State Agencies

In accordance with *Code of Virginia* § 2.2-603, § 2.2-2009 and § 2.2-2005, all State Agencies are responsible for complying with all Commonwealth ITRM policies and standards, and considering Commonwealth ITRM guidelines issued by the Chief Information Officer of the Commonwealth.

Related ITRM Policies, Standards, and Guidelines

- Commonwealth of Virginia Information Technology Security Policy (ITRM Policy SEC500-02)
- Commonwealth of Virginia Information Technology Security Standard (ITRM Standard SEC501-01)

TABLE OF CONTENTS

ITRM PUBLICATION VERSION CONTROL ii
PREFACE iii
1. INTRODUCTION 1
1.1 How to Use this Standard 1
1.2 Definitions1
1.2.1 Commonwealth of Virginia (COV) Information Technology (IT) System 1
1.2.2 Data Communications 1
1.2.3 Data Owner 1
1.2.4 Government Database 1
1.2.5 IT Security Audit 2
1.2.6 IT Security Auditors 2
1.2.7 Sensitive IT Systems and Data 2
1.3 Chief Information Officer (CIO) Designation 2
1.4 IT Security Audits of Government Databases 2
2. PERFORMANCE OF IT SECURITY AUDITS 4
2.1 Planning for IT Security Audits 4
2.2 IT Security Audit Scope 4
2.3 Access Required to Perform IT Security Audits 4
2.4 Performance of IT Security Audits 5
2.5 Documentation of IT Security Audits 5
2.5.1 IT Security Audit Work Papers 5
2.5.2 IT Security Audit Reports 5
2.5.3 Corrective Action Plan Reporting and Verification 6
2.5.4 Reporting IT Security Audit Results to VITA 6
3. GLOSSARY 7

1. INTRODUCTION

1.1 How to Use this Standard

This Standard is written to be read from front to back, as its requirements are interrelated. If the reader tries to consider just one area and skip others, the reader's Agency risks overlooking important requirements and may be unaware of areas in which the Agency does not comply with the Standard. Furthermore, this Standard is written to be read in conjunction with the following two Information Technology (IT) security documents: *Commonwealth of Virginia Information Technology Security Policy* (ITRM Policy SEC500-02) and *Commonwealth of Virginia Information Technology Security Standard* (ITRM Standard SEC501-01).

1.2 Definitions

The roles and responsibilities defined in the *Commonwealth of Virginia Information Technology Security Policy* (ITRM Policy SEC500-02) shall apply to this standard. For the purposes of this standard, the following definitions also shall apply:

1.2.1 Commonwealth of Virginia (COV) Information Technology (IT) System

In general, an IT system is an interconnected set of IT resources under the same direct management control. For the purposes of this standard, a Commonwealth of Virginia (COV) IT system is any such system that processes COV data.

1.2.2 Data Communications

Data Communications includes the equipment and telecommunications facilities that transmit, receive, and validate COV data between and among computer systems, including the hardware, software, interfaces, and protocols required for the reliable movement of this information. As used in this document, Data Communications is included in the definition of government database herein.

1.2.3 Data Owner

The Data Owner is the Agency manager responsible for the policy and practice decisions regarding data.

1.2.4 Government Database

Strictly speaking, a government database is a collection of COV data organized into interrelated tables and specifications of data objects.

For the purposes of this standard, however, the term "government database" shall include all components of any COV IT system in which a database resides, and shall also include state Data Communications, as defined herein. This definition of "government database" applies irrespective of whether the COV information is in a physical database structure

maintained by COV or a third-party provider. However, this definition does not include databases within Agencies that have been determined by the Agencies themselves to be non-governmental.

1.2.5 IT Security Audit

An Information Technology (IT) Security Audit is an independent review and examination of an IT system's policies, records, and activities. The purpose of the IT security audit is to assess the adequacy of IT system controls and compliance with established IT security policy and procedures.

1.2.6 IT Security Auditors

IT Security Auditors are CISO personnel, Agency Internal Auditors, the Auditor of Public Accounts, or a staff of a private firm that, in the judgment of the Agency, has the experience and expertise required to perform IT security audits.

1.2.7 Sensitive IT Systems and Data

Sensitive Data is any data of which the compromise with respect to confidentiality, integrity, and/or availability could adversely affect COV interests, the conduct of Agency programs, or the privacy to which individuals are entitled. Sensitive IT Systems are COV IT systems that store, process, or transmit sensitive data.

For the purposes of this standard, Sensitive IT Systems and Data are any IT system or data classified by the Agency as sensitive in accordance with the requirements of the *Commonwealth of Virginia Information Technology Security Standard* (ITRM Standard SEC501-01), Section 2.5: System and Data Sensitivity Classification.

1.3 Chief Information Officer (CIO) Designation

The Chief Information Officer (CIO) of the Commonwealth has designated the Chief Information Security Officer (CISO) of the Commonwealth to develop policies, procedures, and standards for:

a. Assessing IT security risks;

b. Performing IT security audits of government databases and data communications; and

c. Determining appropriate IT security measures.

1.4 IT Security Audits of Government Databases

Each Agency shall establish an IT Security Audit Program. The program shall include assessing the risks associated with the state government databases for which it is the Data Owner and conducting IT Security Audits at a frequency relative to the risk identified by the Agency. At a minimum, databases that contain sensitive data, or reside in a system with a

sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall be assessed at least once every three years.

2. PERFORMANCE OF IT SECURITY AUDITS

IT Security Audits shall be conducted by personnel or organizations defined as IT Security Auditors in section 1.2.6, above, or by such other entity as approved by the CISO.

2.1 Planning for IT Security Audits

This *Standard* does not require, and shall not be construed to require, duplication of audits already performed or underway, except when it is deemed necessary by auditing entities whose audit rights, by Virginia law, cannot be infringed. Coordinated IT security audit planning is, therefore, essential and shall be the responsibility of the Agency Head or designee.

Annually, each Agency shall develop an IT security audit plan or review and as necessary, update an existing one for the government databases for which it is the Data Owner. The IT security audit plan shall be based on the Business Impact Analysis (BIA) and data classification performed by the Agency. Each Agency Head shall submit the Agency IT security audit plan to the CISO. However, the initial IT security audit plan shall be submitted to the CISO at the Agency's earliest convenience, but not later than 7 months after the effective date of this standard.

If the database relies upon IT services provided by VITA or any other service provider, the IT Security Auditor shall rely on any applicable IT Security Audits performed during the applicable audit cycle for that component of the IT Security Audit. For IT services provided by VITA, the CISO will coordinate the VITA IT security audits. If an Agency has VITA IT security audit needs that are not met through existing or planned IT security audits, the Agency should contact the CISO to address those needs. It is the Agency's responsibility to ensure that adequate IT security audit provisions exist relative to other service providers.

The CISO may also conduct IT Security Audits as circumstances warrant, or upon request of any entity with operational or audit authority over the government database in question.

2.2 IT Security Audit Scope

In conducting IT Security Audits, the IT Security Auditor shall use criteria that, at a minimum, assess the effectiveness of the system controls and measures compliance with the applicable requirements of the *Commonwealth of Virginia Information Technology Security Policy* (ITRM Policy SEC500-02) and the *Commonwealth of Virginia Information Technology Security Standard* (ITRM Standard SEC501-01). IT Security Auditors also should use standards that measure compliance with any other applicable Federal and COV regulations.

2.3 Access Required to Perform IT Security Audits

IT Security Auditors shall be granted all access required to perform IT Security Audits, including logical and physical access on a need-to-know basis.

2.4 Performance of IT Security Audits

Prior to performing each IT Security Audit, the IT Security Auditor will contact the Agency Head or designee and agree on:

- A specific scope, in accordance with Section 2.2 of this standard;
- A mutually agreeable schedule for the IT Security Audit;
- A checklist of information and access required for the IT Security Audit.

After agreeing to a scope, schedule and checklist, the IT Security Auditor will conduct the IT Security Audit.

2.5 Documentation of IT Security Audits

2.5.1 IT Security Audit Work Papers

The IT Security Auditor shall prepare audit work papers as documentation of the audit, including sufficient competent evidential matter to support all conclusions. The IT Security Auditor should take care that such work papers do not constitute an unnecessary security risk and are safeguarded appropriately.

2.5.2 IT Security Audit Reports

The IT Security Auditor will document the findings of the IT Security Audit. Prior to formal presentation of the IT Security Audit Report, the IT Security Auditor will present a draft of the report to the Agency Head or designee. They will discuss the report and make any mutually agreeable changes. The Agency Head or designee shall then be given no less than 10 business days to prepare a Corrective Action Plan ("plan"). The plan shall include concurrence or non-concurrence with each finding in the IT Security Audit Report.

For each finding with which the Agency concurs, the plan shall include the:

a. Planned corrective action;

b. Due date for the corrective action; and

c. Party responsible for the corrective action.

For each finding with which the Agency does not concur, the plan shall include the:

d. Agency's statement of position;

e. Mitigating controls that are in place; and

f. Agency's acknowledgment of its acceptance of risk.

Upon receipt of the plan, the IT Security Auditor shall incorporate the plan in the final IT Security Audit Report and present the final IT Security Audit Report to the Agency Head and the Agency Information Security Officer.

2.5.3 Corrective Action Plan Reporting and Verification

A. Implementation

Until completion of all corrective actions in the plan, the responsible Agency Head or designee shall receive reports, at least annually from the date of the final IT Security Audit Report, on progress toward implementing outstanding corrective actions.

B. Verification

Upon completion of the plan, the responsible Agency Head or designee shall arrange for a follow-up review to verify implementation of the specified corrective actions.

2.5.4 Reporting IT Security Audit Results to VITA

At least once each quarter, each Agency Head or designee shall submit to the CISO a report containing the following information:

1. A record of all IT Security Audits conducted by or on behalf of the Agency during that quarter, including all findings, and whether the Agency concurs or does not concur with each.

2. For each finding with which the Agency concurs:
    a. Corrective action planned;
    b. Due date for the corrective action; and
    c. Party responsible for the corrective action.

3. For each finding with which the Agency does not concur:
    a. Agency's statement of position;
    b. Mitigating controls that are in place; and
    c. Agency's acknowledgment of their acceptance of the risk.

4. Status of outstanding corrective actions for all IT Security Audits conducted by or on behalf of the Agency previously.

3. GLOSSARY

Academic Instruction and Research Systems: Those systems used by institutions of higher education for the purpose of providing instruction to students and/or by students and/or faculty for the purpose of conducting research.

Agency Head: The chief executive officer of a department established in the executive branch of Commonwealth of Virginia.

Application: A computer program or set of programs that meet a defined set of business needs. See also *Application System.*

Application System: An interconnected set of IT resources under the same direct management control that meets a defined set of business needs. See also *Application, Support System,* and *Information Technology (IT) System.*

Availability: The computer security characteristic that addresses requirements for IT systems and data to be operational in support of essential business functions and that measures the sensitivity of IT systems and data to unexpected outages.

Business Function: A collection of related structural activities that produce something of value to the organization, its stakeholders or its customers. See also *Essential Business Function.*

Business Impact Analysis (BIA): The process of determining the potential consequences of a disruption or degradation of business functions.

Chief Information Officer of the Commonwealth (CIO): The CIO oversees the operation of the Virginia Information Technologies Agency (VITA) and, under the direction and control of the Virginia Information Technology Investment Board (the Board), exercises the powers and performs the duties conferred or imposed upon him by law and performs such other duties as may be required by the Board.

Chief Information Security Officer of the Commonwealth (CISO): The CISO is the senior management official designated by the CIO of the Commonwealth to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of COV IT systems and data.

Commonwealth of Virginia (COV): The Executive Branch of the government of the Commonwealth of Virginia, or its Agencies or departments.

Confidentiality: The computer security characteristic that addresses requirements that data is disclosed only to those authorized to access it, and that measures the sensitivity of data to unauthorized disclosure.

Council on Technology Services (COTS): An advisory council that assists in the development of a blueprint for state government IT planning and decision-making. The Council advises the Chief Information Officer of the Commonwealth on the services provided by the Virginia Information Technologies Agency (VITA) and the development and use of applications in state agencies and public institutions of higher education.

Data: Data consists of a series of facts or statements that may have been collected, stored, processed and/or manipulated but have not been organized or placed into context. When data is organized, it becomes information. Information can be processed and used to draw generalized conclusions or knowledge.

Database: A database is a collection of data organized into interrelated tables and specifications of data objects.

Data Classification: A process of categorizing data according to its sensitivity.

Data Communications: Data Communications includes the equipment and telecommunications facilities that transmit, receive, and validate COV data between and among computer systems, including the hardware, software, interfaces, and protocols required for the reliable movement of information. As used in this document, Data Communications is included in the definition of government database, herein.

Data Custodian: An individual or organization in physical or logical possession of data for Data Owners. Data Custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage and for providing and administering general controls, such as back-up and recovery systems.

Data Owner: An Agency Manager responsible for the policy and practice decisions regarding data. For business data, the individual may be called a business owner of the data.

Data Security: Data Security refers to those practices, technologies, and/or services used to apply security appropriately to data.

Essential Business Function: A business function is essential if disruption or degradation of the function

prevents the Agency from performing its mission as described in the Agency mission statement.

Evaluation: Investigative and test procedures used in the analysis of security mechanisms to determine their effectiveness and to support or refute specific system weaknesses.

Government Database: For the purposes of this document, the term "government database" includes both databases that contain COV data and data communications that transport COV data. This definition applies irrespective of whether the COV information is in a physical database structure maintained by COV or a third-party provider. However, this definition does not include databases within Agencies that have been determined by the Agencies themselves to be non-governmental. See also *Database* and *Data Communications.*

Information Security Officer (ISO): The individual who is responsible for the development, implementation, oversight, and maintenance of the Agency's IT security program.

Information Technology (IT): Telecommunications, automated data processing, databases, the Internet, management information systems, and related information, equipment, goods, and services.

Information Technology (IT) Security: The protection afforded to IT systems and data in order to preserve their availability, integrity, and confidentiality.

Information Technology (IT) Security Audit: An independent review and examination of an IT system's policy, records, and activities. The purpose of the IT security audit is to assess the adequacy of IT system controls and compliance with established IT security policy and procedures.

Information Technology (IT) Security Auditor: CISO personnel, Agency Internal Auditors, the Auditor of Public Accounts, or a private firm that, in the judgment of the Agency, has the experience and expertise required to perform IT security audits.

Information Technology (IT) Security Controls: The protection mechanisms prescribed to meet the security requirements specified for an IT system. These mechanisms may include but are not necessarily limited to: hardware and software security features; operating procedures, authorization and accountability access and distribution practices; management constraints; personnel security; and environmental and physical safeguards, structures, and devices. Also called IT security safeguards and countermeasures.

Information Technology (IT) Security Safeguards: See *Information Technology (IT) Security Controls*.

Information Technology (IT) System: An interconnected set of IT resources under the same direct management control. See also *Application System* and *Support System.*

Integrity: The computer security characteristic that addresses the accuracy and completeness of IT systems and data, and that measures the sensitivity of IT systems and data to unauthorized or unexpected modification.

Least Privilege: The minimum level of data, functions, and capabilities necessary to perform a user's duties. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an IT system.

Non-sensitive Data: Data of which the compromise with respect to confidentiality, integrity, and/or availability could not adversely affect COV interests, the conduct of Agency programs, or the privacy to which individuals are entitled.

Personnel: All COV employees, contractors, and subcontractors, both permanent and temporary.

Residual Risk: The portion of risk that remains after security measures have been applied.

Risk: The possibility of loss or injury based on the likelihood that an event will occur and the amount of harm that could result.

Risk Assessment (RA): The process of identifying the vulnerabilities, threats, likelihood of occurrence, potential loss or impact, and theoretical effectiveness of security measures. Results are used to evaluate the level of risk and to develop security requirements and specifications.

Risk Mitigation: The continuous process of minimizing risk by applying security measures commensurate with sensitivity and risk.

Secure: A state that complies with the level of security controls that have been determined to provide adequate protection against adverse contingencies.

Sensitive Data: Any data of which the compromise with respect to confidentiality, integrity, and/or availability could adversely affect COV interests, the conduct of Agency programs, or the privacy to which individuals are entitled.

Sensitive IT Systems: COV IT systems that store, process, or transmit sensitive data.

Sensitivity Classification: The process of determining whether and to what degree IT systems and data are sensitive.

Separation of Duties: Assignment of responsibilities such that no one individual or function has control of an entire process. Implied in this definition is the concept that no one person should have complete control. Separation of duties is a technique for maintaining and monitoring accountability and responsibility for IT systems and data.

State: See *Commonwealth of Virginia (COV).*

Support System: An interconnected set of IT resources under the same direct management control that shares common functionality and provides services to other systems. See also *Application System* and *Information Technology (IT) System.*

System. See *Information Technology (IT) System*

System Owner: An Agency Manager responsible for the operation and maintenance of an Agency IT system.

Technology Strategy and Solutions (TSS): A directorate within VITA; the publisher of all VITA external and internal policies, standards, and guidelines. TSS develops architectural standards and the accompanying policies and procedures for the enterprise, and advises the CIO on architectural standards and exceptions. It also tracks emerging trends and best practices across the spectrum of technologies, including hardware, operating systems, networking and communications, security, and software applications.

Third-Party Provider: A company or individual that supplies IT equipment, systems, or services to COV Agencies.

Threat: Any circumstance or event (human, physical, or environmental) with the potential to cause harm to an IT system in the form of destruction, disclosure, adverse modification of data, and/or denial of service by exploiting vulnerability.

Virginia Information Technologies Agency (VITA): VITA is the consolidated, centralized IT organization for COV.